NxtAssets Compliance Matrix

Mapping NxtAssets to TX Election Code, EAC Best Practices & CISA Guidance

For Election Administrators and Compliance Officers

NxtElections, Inc. | April 2026

Texas election administrators operate under a layered regulatory framework mandating strict chain of custody, tamper-evident seal management, real-time asset tracking, and immutable audit records for all voting equipment and materials. NxtAssets was purpose-built to meet these requirements. The table below maps each regulatory mandate to the specific NxtAssets capability that addresses it.

Compliance Domain	Regulatory Citation	Source	Requirement Summary	NxtAssets Capability	How NxtAssets Addresses the Requirement
Pre-Election Security & Inventory	TEC §129.051(a)	TX Election Code	General custodian shall create and maintain an inventory of all electronic information storage media.	Asset Registry; Multi-Identifier Tracking	NxtAssets maintains a central asset registry supporting multiple identifier types per asset (manufacturer serial, county barcode, RFID tag, BLE beacon, GPS tracker). Asset Types allow flexible classification with custom attributes. System runs on Oracle 23ai and handles 50K+ assets.
Pre-Election Security & Inventory	TEC §129.051(b)	TX Election Code	Develop procedure for tracking custody of each storage medium from storage through election coding, election process, to post-election disposition and return. Chain of custody requires two or more individuals at each transfer.	Chain-of-Custody Module; Dual-Signature Capture; Configurable Workflows	Every custody handoff captures: both parties' names/IDs, digital signatures on mobile device, timestamp, GPS location, device/network metadata, and event type. Stored in Oracle immutable (blockchain) table — cannot be altered or deleted even by a DBA. Workflows model the full lifecycle from storage → coding → deployment → return → post-election disposition.
Pre-Election Security & Inventory	TEC §129.051(c)	TX Election Code	Establish a secured location for storing electronic storage media when not in use, during coding, during transfer/installation into equipment, and after election parameters are loaded.	Location Management; Geo-Fencing; BLE Warehouse Mesh	NxtAssets tracks asset locations in real time via GPS/BLE/RFID. A mesh of BLE beacons and WiFi access points within the warehouse pinpoints assets to shelf/station level. Geo-fence boundaries trigger alerts on unauthorized departures. Workflow states (e.g., 'In Secure Storage,' 'In Coding,' 'Parameters Loaded') enforce proper transitions.
Pre-Election Security & Inventory	TEC §129.051(d)	TX Election Code	Election information storage medium shall be kept in the presence of an election official or in a secured location once coded for an election.	Continuous Asset Monitoring; Presence Detection	BLE beacon presence detection confirms whether coded media remain within designated secure zones. GPS trackers on configurable sync intervals (active: 30 sec, idle: 1 hr) monitor assets at rest. Departure from secure zone triggers real-time alert to designated personnel.
Pre-Election Security & Inventory	TEC §129.051(f)	TX Election Code	Create a recovery plan for security breaches, including immediately notifying the Secretary of State.	Real-Time Alerting; Immutable Audit Trail; Incident Workflows	Geo-fence deviation alerts, unexpected seal-break events, and asset separation alerts provide immediate detection. Immutable audit trail provides forensic evidence for breach investigation. Custom incident-response workflows can be configured to include SOS notification as a mandatory step.
Pre-Election Security & Inventory	TEC §129.051(g)	TX Election Code	Conduct criminal background checks for relevant election officials, staff, and temporary workers upon hiring.	Role-Based Access Control (RBAC); OCI IAM	Background checks are an HR process external to NxtAssets. The system enforces the outcome: only provisioned users access the system. RBAC and ABAC in APEX and OCI IAM restrict operations by role. All user actions are audit-logged with user identity, timestamp, and device metadata.

Compliance Domain	Regulatory Citation	Source	Requirement Summary	NxtAssets Capability	How NxtAssets Addresses the Requirement
Transport & Custody of Equipment	TEC §129.052(a)	TX Election Code	Adopt procedures for securely storing and transporting voting system equipment. Must include overnight storage at polling locations. Chain of custody requires two or more individuals at each transfer.	Work Orders; Delivery Workflows; GPS Tracking; Dual-Signature Chain of Custody	NxtAssets models the complete transport lifecycle via Work Orders: warehouse loading → delivery → polling-site overnight → return. GPS trackers on vehicles provide in-transit visibility. Dual digital signatures enforced at every custody transfer. Geo-fences validate correct delivery destinations. Work Order status tracks actual vs. planned handling to identify discrepancies (e.g., equipment dropped at wrong location).
Transport & Custody of Equipment	TEC §129.052(b)	TX Election Code	Create a recovery plan for transport security breaches, including immediately notifying the Secretary of State.	Geo-Fence Deviation Alerts; Asset Separation Alerts; Configurable Incident Workflows	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 SOS notification as a required step, with the event documented in the immutable audit trail.
Transport & Custody of Equipment	TEC §129.052(c)	TX Election Code	Provide a training plan for relevant election officials, staff, and temporary workers addressing transport security procedures.	Workflow-Embedded SOPs; Formal Training Program	NxtAssets workflows act as embedded SOPs — the system guides users through required steps and prevents skipped actions. NES provides formal instructor-led training: System Admins (1.5–2 days), Warehouse & Field Staff (½ day), Election Site Leads (½ day), IT & Reporting (½ day), Service Desk (2 hrs). Refresher sessions before major elections.
Access to Voting Equipment	TEC §129.053	TX Election Code	Secure access control keys/passwords to voting system equipment. Use must be witnessed and documented in a dedicated log retained until equipment is disposed.	RBAC/ABAC; Immutable Activity Logs; Definable Retention Policies	NxtAssets provides role-based and attribute-based access controls via 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 equipment lifecycle.
Seal Management	TEC §129.024(a)	TX Election Code	On completing each test, place test materials in a sealed container. Custodian and at least two testing board members shall sign the seal.	Seal Tracking Module; Workflow-Enforced Seal Steps; Multi-Party Sign-Off	NxtAssets tracks every seal by unique serial number and type (tamper-evident, plastic, padlock). L&A testing workflows include mandatory seal-application steps that cannot be bypassed. Records which seal ID goes on which container, who applied it, and when. Multi-party chain-of-custody signatures capture the dual+ witness requirement.
Seal Management	TEC §129.024(b)–(c)	TX Election Code	Test materials remain sealed for the preservation period. May not be unsealed except for authorized proceedings. If unsealed, must be resealed when not in use.	Seal Status Tracking; Immutable Seal Event Log; Configurable Retention Policies	Every seal event (apply, inspect, remove, reapply) 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)).
Seal Management	TEC §127.064	TX Election Code	Seals for ballot boxes must be serially numbered.	Serialized Seal Registry	NxtAssets maintains a registry of all seals by serial number and type. Seal Types are configurable. Barcode scanning of seal serial numbers ensures accurate association with the correct ballot box or asset.

Compliance Domain	Regulatory Citation	Source	Requirement Summary	NxtAssets Capability	How NxtAssets Addresses the Requirement
Seal Management	TEC §§127.065–.066	TX Election Code	Seal ballot boxes before delivery to polling places. Seal deposit slot at close of voting. Deliver sealed ballot boxes to Central Counting Station.	Workflow-Enforced Seal Checkpoints at Each Phase	Election workflows include mandatory seal-application steps at each statutory checkpoint: before delivery, at poll close, and before CCS transport. 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. The system knows required sealing points on each asset type.
Equipment Prep, Delivery & Installation	TEC §§125.002–.004	TX Election Code	Prepare equipment before delivery. SOS-prescribed delivery procedures to prevent tampering/damage. Installation procedures to protect equipment at polling places.	Work Orders with BOM/Configurator; Delivery Workflows; Setup Checklists	Work Orders drive equipment prep with checklists (diagnostic test, firmware update, seal application). Product Configurator generates context-specific Bills of Materials per location type (standard, ADA-enhanced, high-capacity, early voting). Delivery workflows track loading, transit, and handoff. Setup workflows at polling locations include inspection checklists before opening.
Polling Place Security & Closeout	TEC §125.005	TX Election Code	Presiding judge shall periodically inspect voting system equipment for tampering and damage during voting.	Seal Audit Function; Mobile Inspection Interface	NxtAssets supports routine seal audits on any mobile device via web browser: pull up the asset, view expected seals (by serial number and seal point), inspect physical seals, log ‘audit pass’ or ‘audit fail’ with timestamp. Failed audits trigger immediate alerts to administrators. Complete seal audit history maintained per asset.
Polling Place Security & Closeout	TEC §125.063	TX Election Code	On close of voting, an election officer shall secure or inactivate equipment to prevent unauthorized operation.	Close-Poll Workflow; Seal Application Steps; Equipment Status Transition	NxtAssets provides a ‘Close Poll’ workflow enforcing all required closeout steps in sequence: seal application, equipment lockdown, packing, custody transfer recording. Status transitions from ‘In Use at Polling Location’ to ‘Closed Out’ require completion of all checklist items.
Polling Place Security & Closeout	TEC §125.064	TX Election Code	Documents/records used in or generated by the electronic voting system shall be available for public inspection during the retention period.	Exportable Reports; Immutable Records; Retention Policies	NxtAssets provides predefined customizable reports exportable as CSV. Document-formatted reports via Word templates. Natural language query tool for ad-hoc reports. Immutable tables with configurable retention policies ensure records persist for the required period.
Precinct Records & Retention	TEC §66.021	TX Election Code	Assemble and seal precinct records in specified envelopes; lock boxes for distribution.	Asset Nesting; Seal Tracking on Containers	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 maintained so the system knows which items were in which containers at any point.
Precinct Records & Retention	TEC §66.058	TX Election Code	Preserve precinct records 22 months. Voted ballots in locked room and locked box. Electronic records from Ch. 129 in a secure container. Offenses for unauthorized entry.	Immutable Audit Trail with 22-Month Retention; Secure Location Tracking	Oracle immutable tables support definable retention policies set to statutory 22-month minimum. Physical asset location tracked continuously via BLE/GPS — system detects if a sealed container leaves designated secure storage. Access control logs document who accessed which container and when.
Precinct Records & Retention	TEC §66.062	TX Election Code	Follow directions on storage/return of boxes, keys, booths, and other equipment.	Return Workflows; Rally Point Check-In; Reconciliation Reports	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. Highlights discrepancies between planned and actual returns.

Compliance Domain	Regulatory Citation	Source	Requirement Summary	NxtAssets Capability	How NxtAssets Addresses the Requirement
CCS Program & Equipment IDs	TEC §§127.123, 127.154–.155	TX Election Code	Protect tabulation program. Assign permanent IDs to tabulators and parts. Record on ballot-and-seal certificates. Presiding judge signs tabulation tapes.	Permanent Asset IDs; Multi-Identifier Registry; Signature Capture	NxtAssets assigns permanent identifiers to every asset (tabulator, parts, 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.
EAC: Chain of Custody	EAC Best Practices: Chain of Custody (2021)	EAC	At least two signatures on each custody transfer. Record: detailed description of item, seal numbers, party names, date/time, location, signatures.	Dual-Signature Chain-of-Custody Events	NxtAssets custody events capture all EAC-recommended data points: both parties' names/IDs, digital signatures, timestamp, GPS location, event type/reason, and notes (including seal numbers). Dual-party requirement enforced by workflow — event not logged until both signatures captured.
EAC: Chain of Custody	EAC Best Practices: Chain of Custody (2021)	EAC	Written chain-of-custody procedures available for public inspection prior to every election. Review and update after each election.	Configurable Workflow Engine; Exportable Process Definitions	Workflow definitions stored in JSON, mappable to BPMN. Processes can be exported, documented, and made available for inspection. Configurable engine allows post-election review and updates without coding — new steps, approvals, or verification requirements added via admin interface.
EAC: Chain of Custody	EAC Best Practices: Chain of Custody (2021)	EAC	Documentation at multiple points during tabulation. Tamper-evident seal usage recommended. Multiple documentation checkpoints advised.	Seal Management; Multi-Point Workflow Checkpoints; Immutable Logs	Configurable seal types including tamper-evident seals. Workflows include multiple seal-check and chain-of-custody checkpoints throughout the election cycle (pre-delivery, delivery, setup, close, return, tabulation). All events immutably logged.
EAC: Physical Security	EAC Best Practices for Election Technology	EAC	Physical security safeguards required in storage, transit, polling place, during voting, and through post-election. Includes chain of custody, tamper-evident seals, limiting access, two-person accountability, access logging.	End-to-End Lifecycle Tracking; Seal Management; Access Logging; Dual-Party Transfers	Continuous tracking warehouse through every phase to post-election. Tamper-evident seal tracking with serial numbers. All user actions logged immutably. Dual-signature custody enforced. GPS/BLE monitoring in storage and transit. RBAC limits access.
EAC: Equipment Management	EAC Disposal of Election Equipment (Inventory BMPs)	EAC	Maintain: equipment checkout tracking, usage history per election, maintenance history, repair history, disposal records.	Asset Lifecycle Tracking; Status History; Maintenance/Repair Logging	NxtAssets tracks each asset's complete lifecycle: current and historical location, status history, workflow history, nesting history, seal history, Work Order history. Status states include New, Available, In Use, Watch, Replaced, Certified, Tabulated. Maintenance/repair events logged per asset.
CISA: CoC Framework — Identify	CISA Insights: Chain of Custody and Critical Infrastructure Systems (2021)	CISA	IDENTIFY: Identify critical assets. Inventory all systems, devices, software, data, and people. Document logs that track transactions and access. Routinely assess logs for gaps.	Asset Registry; Multi-Identifier Inventory; Activity Logs; Gap Detection	Complete inventory of all election assets with multiple identifiers. All transactions logged. Reconciliation reports compare planned vs. actual handling to surface gaps. Dashboards show real-time status highlighting incomplete or overdue items.
CISA: CoC Framework — Protect	CISA Insights: Chain of Custody and Critical Infrastructure Systems (2021)	CISA	PROTECT: Implement physical and electronic access control. Authorize only appropriate individuals. Continuous monitoring. Manage records for confidentiality, integrity, availability.	RBAC/ABAC; Immutable Audit Trail; Continuous GPS/BLE Monitoring; Encrypted Data	RBAC and ABAC via APEX and OCI IAM. TLS in transit; TDE at rest. Immutable blockchain tables for critical records. Continuous GPS/BLE monitoring of physical assets. Hosted on OCI FedRAMP Government Cloud.
CISA: CoC Framework — Detect	CISA Insights: Chain of Custody and Critical Infrastructure Systems (2021)	CISA	DETECT: Develop activities to identify chain-of-custody breaches. Detective measures identify anomalies and unauthorized access.	Geo-Fence Alerts; Seal-Break Detection; Dashboard Anomaly Visibility	Real-time alerts on: geo-fence departures, unexpected asset movements, seal integrity failures, Work Order discrepancies (wrong item at wrong location). Dashboards highlight late, missing, or mis-delivered assets.

Compliance Domain	Regulatory Citation	Source	Requirement Summary	NxtAssets Capability	How NxtAssets Addresses the Requirement
CISA: CoC Framework — Respond	CISA Insights: Chain of Custody and Critical Infrastructure Systems (2021)	CISA	RESPOND: Execute response processes. Document incidents. Sanitize media per NIST SP 800-88. Review hardware for unauthorized modification.	Incident Documentation via Immutable Trail; Configurable Response Workflows	Immutable audit trail provides forensic-quality incident documentation. Custom response workflows configurable. Seal audit function detects hardware modifications. Records exportable as evidence for investigations, court proceedings, FOIA.
CISA: CoC Framework — Recover	CISA Insights: Chain of Custody and Critical Infrastructure Systems (2021)	CISA	RECOVER: Restore systems from validated versions. Recertification may be needed for affected systems.	Asset Status Tracking; Equipment Swap Workflows; History for Recertification	Complete history of each asset enables auditors to determine breach scope. Equipment swap workflows document replacement of compromised assets. 'Quarantine' status isolates affected equipment. Full history export supports recertification review by SOS or EAC.
TX SOS Advisory Compliance	TX SOS Advisory 2019-23 §9	TX SOS	Secure storage must employ uniquely identified tamper-resistant/tamper-evident seals and logs. Create and maintain seal inventory per storage location per election. Two or more individuals required at every custody transfer or when equipment has been left unattended.	Seal Registry with Location Tracking; Dual-Party Transfers; Per-Election Seal Inventory	Complete seal registry by type, serial number, and current association (asset, seal point, location). Per-election seal inventory via reports. Dual-party custody enforced at every transfer. BLE/GPS detects when equipment has been unattended outside designated zones.
TX SOS Advisory Compliance	TX SOS Advisory 2019-23 (Seal Checks During Voting)	TX SOS	Election official shall periodically check for evidence of tampering on voting equipment during the election — e.g., verify seal is still intact. (Per TEC §125.005.)	Mobile Seal Audit Interface; Real-Time Seal Status Reporting	Poll workers or roving technicians perform seal audits on mobile device: scan asset, view expected seals (serial number + seal point), inspect physical seals, log pass/fail. Failed audits surface in dashboards and trigger alerts. Complete audit history maintained per asset.
TX SOS Advisory Compliance	TX SOS Advisory 2019-23 (Recovery Plan)	TX SOS	Written recovery plan must address inadvertent seal damage and custody documentation errors. Plans must enhance public confidence. Breach/error/seal damage indications must be confirmed by more than one individual.	Multi-Person Verification; Incident Logging; Public-Facing Audit Reports	Dual-signature requirements enforce multi-person confirmation. Seal damage events logged with cause codes and verified by second party. Incident events immutably recorded. Exportable audit reports support public transparency. Reports available for FOIA or observer review.
NIST Framework Alignment	NIST CSF (referenced by CISA for election infrastructure)	NIST/CISA	CISA recommends election infrastructure owners use NIST Cybersecurity Framework. Five functions: Identify, Protect, Detect, Respond, Recover.	Full NIST CSF Function Coverage	NxtAssets maps to all five functions: IDENTIFY (asset inventory, multi-ID registry), PROTECT (RBAC, encryption, immutable logs), DETECT (geofence alerts, seal audit, anomaly dashboards), RESPOND (incident workflows, forensic trail), RECOVER (quarantine status, swap workflows, history export for recertification).