Precinct Central Security Overview

System Configuration Overview

Precinct Central is a modern election platform which unites the industry's most secure technology with best-in-class functionality. System components, including software, hardware, and security are recognized nationwide as the benchmark in election administration.

Configuration Management Plan

- **Mobile Device Management:** Tenex ensures all systems are consistent and up-to-date as a vital component of election security. The mobile device management (MDM) platform secures these updates so they are centrally controlled and audited.

- **Application Control:** Counties must white-list application used on the device, therefore, only the *Precinct Central* electronic poll book application, and those associated apps are installed on the iPad. The device is fully locked down, and no other applications can be installed other than those white-listed through the MDM platform.

- **Security and Configuration Policy Enforcement:** Through MDM, each device is configured to use identical configuration policies and provide a consistent experience for pollworkers. This means all security settings, including device names, network names, and passwords are configured and fully auditable via the MDM.

- **Remote Lock and Lost Mode Security:** The remote lock feature allows fully locking down the device. For a lost device, the lost mode functionality can be used to remotely lock the iPad or wipe it completely. Devices can also be tracked on a map to discover the last known approximate GPS location for the device.

FIPS compliant Apple iPad platform

Apple is one of the few mobile tablet vendors satisfying the strict FIPS 140-2 specification for security. The Federal Information Processing Standards (FIPS) are standards specified by the United States Government for approving cryptographic software. The National Institute of Standards and Technology (NIST) has so far issued the FIPS 140-1 and FIPS 140-2 standards, and FIPS PUB 140-2 is the standard for "Security Requirements for Cryptographic Modules."

Amazon Web Service (AWS) platform

Precinct Central is secured via the AWS platform's data and application hosting. As part of the AWS service agreement, Amazon provides an infrastructure for physical hardware security, networking infrastructure, and virtualization infrastructure.

Center for Internet Security (CIS) Security Benchmarks

Precinct Central employs CIS security benchmarks for server hardening and vulnerability checklists. Developed by an international community of cybersecurity experts, the CIS Benchmarks provide guidelines for establishing a secure configuration posture for IT Infrastructures.