acet
AMERICAN COUNCIL FOR ELECTION TECHNOLOGY

SECURITY BEYOND VOTING SYSTEMS

Protecting the Technology that Supports Elections



Many supporting election technologies connect to the internet, handle sensitive information, or face heavy demand. This includes voter registration databases and online portals, electronic ballot transmission systems, and election night reporting websites. ACET members use layered safeguards, independent testing, and continuous monitoring to protect these services.

ACET MEMBER PRIORITIES

SECURITY

Prevent unauthorized access, cyberattacks, and system misuse.

CONFIDENTIALITY & PRIVACY

Protect sensitive voter information and ballot privacy, where applicable.

INTEGRITY

Keep voter records, ballot information, and reported results accurate; detect and trace unauthorized changes.

AVAILABILITY

Maintain service during heavy traffic, outages, and cyberattacks.

HOW ACET MEMBERS PROTECT ELECTION TECHNOLOGY

ACCESS & DATA PROTECTION

- Require multi-factor authentication (MFA) and role-based permissions.
- Encrypt sensitive data in transit and at rest.
- Restrict access to protected records.
- Separate public-facing and administrative systems.
- Log access and changes.

SECURE DEVELOPMENT & TESTING

- Review code and software updates.
- Scan for vulnerabilities.
- Conduct independent penetration tests.
- Track software components.
- Apply recognized NIST and ISO standards.

CONTINUOUS MONITORING & INCIDENT RESPONSE

- Monitor security events around the clock.
- Use automated threat detection.
- Maintain and practice incident response and recovery plans.
- Coordinate with election officials when problems arise.

AVAILABILITY & RESILIENCE

- Use hardened cloud infrastructure, including AWS and Microsoft Azure.
- Build in redundancy.
- Test backups and recovery.
- Deploy traffic filtering and DDoS protections.
- Test performance under heavy demand.

INDEPENDENT TESTING & VERIFICATION

SOC 2 TYPE II

An independent examination under AICPA standards evaluates whether specified controls operated effectively over time. Depending on scope, it covers security, availability, processing integrity, confidentiality, and privacy.

RABET-V

Verifies the security, architecture, reliability, and development practices of election-supporting technologies, with risk-based reviews as products change.

EAC ELECTION SUPPORTING TECHNOLOGY EVALUATION PROGRAM (ESTEP)

The EAC's federal certification program currently covers electronic poll books. Requirements for voter registration, electronic ballot delivery, and election night reporting are under development.

ISO & NIST FRAMEWORKS

ISO/IEC 27001 guides information security risk management. NIST frameworks and Special Publication 800 series guide access controls, system protection, monitoring, and incident response.

SECURITY IN PRACTICE

Voter Registration Databases and Systems

Access controls, encryption, audit logs, and recovery procedures protect personal information, restrict record changes, and help preserve accurate voter data.

Electronic Ballot Transmission

Authentication and security controls protect electronic ballot delivery and correct ballot styles. Electronic return, where permitted, is protected by encryption, monitoring, and access controls.

Election Night Reporting

Access controls and audit logs protect unofficial results. Cloud infrastructure, content delivery networks, and DDoS defenses help websites remain accessible during heavy traffic.

A reporting website does not count ballots. An outage, incorrect display, or attempted cyberattack does not itself change underlying vote totals.