



SECURITY FACT SHEET

ExpressVote® 3

Universal Voting System

The purpose-built, paper-based ExpressVote 3 maintains the highest levels of physical and digital security controls. As a Voluntary Voting Systems Guidelines (VVSG) 2.0-compatible device, it provides voter confidence with on-screen, printed and audio playback options for vote selection verification. The unit's security features control access to critical system components.



Physical and System Access Controls

- The ExpressVote 3 is designed to protect against tampering with pick-resistant keylocks and security seals, including during system storage, transport and voting.
- All users must enter security codes when executing administrative and election functions on the ExpressVote 3, such as accessing advanced settings and loading an election.
- The front of each unit includes an inactive slot for a smart card, which will be implemented in a future release to support multifactor authentication.



System Application Controls

- System functions are executable only during election events, in the manner and order intended by election officials performing their duties.
- The system performs a self-diagnostic test at startup, which provides status and alerts election officials of errors.
- The ExpressVote 3 uses Secure Boot and application allowlisting, which verify only the certified operating system, software and firmware are on the unit. For more information about these security features, see *Secure Boot & Application Allowlisting Security Fact Sheet*.
- Only approved and certified components, such as USB flash drives, are accepted by the ExpressVote 3. This prevents any unauthorized data transfers or uploads on the unit.



Encryption, Hash Validation and Digital Signatures

- Election programming is stored on the system as an encrypted and digitally signed data bundle. Each time data is used, a hash validation is performed to ensure data integrity remains intact.
- Administrators can also validate the unit's firmware directly on the unit. This function checks that every file on the operating system is exactly as was written during the Trusted Build by the Voting Systems Test Laboratory (VSTL).



Audit Logs

- The ExpressVote 3 generates a detailed audit log, which can be exported for review and analysis, of all actions and events that have occurred on the unit.
- Every action and event — including access attempts, access of system functions and errors — is logged and time-stamped. The audit log is digitally signed each time an event is recorded.

ExpressVote Auditing

Paper Ballot Card

- Provides a verifiable paper vote record for every voter, containing both human-readable selections and corresponding machine-readable barcodes
- Can be read by any ExpressVote 3 unit before tabulation to verify the voter's intent was captured accurately



Is the Paper from the ExpressVote 3 Auditable?

Yes. Just as hand-marked paper ballots can be inspected or audited by hand or by machine, so can ballot cards. A ballot card contains the same data as a hand-marked ballot, displayed in different ways. During a post-election hand-count audit, selected candidate names are used to count the vote.

ES&S fully supports the use of paper ballots and post-election audits to ensure accuracy and increase confidence in our country's election process. ES&S views paper records as critical for auditing. A physical paper record of the selected candidate names provides the means to a statistically valid post-election audit.

ES&S Security Philosophy

Nothing is more important to ES&S than protecting America's democracy by supporting secure, accessible and accurate elections. That's why every ES&S product reflects our three-part security philosophy:

- **Design:** All products are designed, without compromise, to meet the latest and ever-evolving standards in security, accuracy and reliability.
- **Testing:** In addition to ES&S testing protocols, all tabulation systems are rigorously tested and certified by the federal Election Assistance Commission (EAC), which reflects security and performance standards developed by scientists, academics and election officials. ES&S also takes security testing to the next level, executing penetration testing with independent, accredited laboratories. ES&S submitted our end-to-end voting configuration for Cybersecurity and Infrastructure Security Agency (CISA) critical product evaluation (CPE) at one of our nation's leading research labs.
- **Implementation:** The entire ES&S team is devoted to ensuring that each piece of technology performs as expected on Election Day, helping election officials uphold the laws of their jurisdiction, which mandate strict physical security and tight chain of custody of all voting machines.

Perhaps most importantly, ES&S' essence — its very being — is predicated on supplying America with equipment and software for secure, accurate and accessible elections. All of us at ES&S hold ourselves and each other accountable for this mandate and are proud to serve a role in this noble purpose.