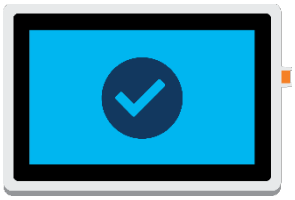
SECURITY FACT SHEET

ExpressPoll®

Electronic Pollbook

ExpressPoll is an application that runs on an enterprise-class Microsoft® Surface Go tablet and displays voter registration data to perform voter search, verification and ballot issuance during an election event. ExpressPoll includes many security features that allow all aspects of the application to be protected, including the physical pollbook devices and the voter registration data.



System Application Controls

ExpressPoll runs on a hardened tablet. Depending on the device and release, this tablet comes pre-installed with either Windows 10 or Windows 11 and the ExpressPoll application that is approved for use in the jurisdiction. Besides ExpressPoll, no application can be installed or started on the tablet, and all unnecessary services and programs, including web browsers, are disabled or uninstalled. This locked-down configuration of the tablet prevents potentially disruptive updates. In addition, each tablet utilizes the following security services:

- Cryptographic functions of the Trusted Platform Module (TPM) 2.0 chip within the motherboard
- A dedicated microcontroller to secure the tablet with integrated cryptographic keys
- Secure Boot, Microsoft's BitLocker Encryption and AppLocker allowlisting technologies to detect and resist tampering of the trusted Windows operating system
- Windows Defender to regularly protect against malware (malicious software) and viruses

Physical and System Access Controls

- ExpressPoll uses role-based security to manage access to features in the application and restrict sensitive functions to specific user roles.
- The ExpressPoll Terminal, Flip stand and their dedicated cases provide physical protection to the ExpressPoll tablet during storage, transport and typical use. Both cases can be further secured with locks and tamper-evident seals.

Secure Data Controls

- All data stored and accessed on the tablet is secured with AES-256 encryption and is password protected. Running code-obfuscating software reduces the risk of the data being decompiled and reverse engineered. If an ExpressPoll tablet is unlawfully removed from a polling location, election officials can protect data from the unit remotely.
- Data is securely transferred between pollbooks and, if configured, to a host server using AES-256 encryption. For pollbook devices to exchange voter data, the devices must be programmed with the same election, which prevents data contamination from other devices.
- Sharing information between a jurisdiction's ExpressPoll tablets, such as when voters are identified and issued a ballot, ensures that no voter is able to vote twice.
- Neither the tablet nor the ExpressPoll application houses sensitive voter data, such as social security or driver's license numbers. By default, poll workers must search for a voter by last name, first name, date of birth, voter address or voter party.

Network Security

- The ExpressPoll tablet cannot connect to unsecured wireless networks, such as public networks that don't require passwords, and requires a minimum of WPA2 wireless security. Also, the tablet does not use Bluetooth® technology.
- ExpressPoll is fully functional in an offline mode. This means network connectivity — whether with other tablets in the jurisdiction or with a host server — is not mandatory.
- When the ExpressPoll tablet connects to a secure network, data synchronizes with peers or the host server without interruption.

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**: ES&S 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, all of us at ES&S are dedicated to supplying America with equipment and software for secure, accurate and accessible elections. We hold ourselves and each other accountable for this mandate and are proud to serve a role in this noble purpose.