



SECURITY BULLETIN

Modeming

Unofficial Results Transmission

Where approved by state election authorities, certain ES&S tabulation systems support the transmission of encrypted unofficial results data through a private, secure wireless network. ES&S adds an extra layer of security through the use of an industry-standard Secure File Transfer Protocol (SFTP). The SFTP, which is used by many Fortune 500 companies, establishes an authenticated and secure connection between the DS200 and the central site communications host, allowing encrypted and digitally-signed unofficial results to be securely transferred to the central reporting location after polls close.

This results transmission methodology, which employs the latest technology and most secure features offered by wireless carrier providers, does not use the public internet and is isolated from all public networks, virtually eliminating security risks associated with malware, viruses, spyware, worms and denial of service attacks.

This optional results transmission methodology is for UNOFFICIAL results reporting only. Official results are obtained through a manual upload to the election management system and canvas performed by election officials at the central reporting location.

SECURING VOTING SYSTEMS

ES&S voting systems are designed and built with multiple layers of protection, including physical controls, system hardening and data integrity validation. Each system generates a detailed audit log of all actions and events that have occurred on the unit for post-election review.

ES&S products employ AES-256 encryption standard and digital signatures for all data-in-transit using industry-standard cryptographic modules that have been validated by the NIST Cryptographic Module Validation Program (CMVP).

Each DS200 configured with modeming technology is assigned unique and election-specific credentials that must pass validation parameters when connecting and authenticating with the back-end communications host. Additionally, the communications host is configured to meet the requirements of the FIPS 140-2 standard and provides an additional layer of encryption during the transfer. This transfer of unofficial election results between the DS200 and back-end central reporting location happens after the polls close.

MODEM ACTIVATION RESTRICTIONS

The DS200's optional wireless modem is only activated after polls close and results are printed from each DS200 on election night. When user credentials are authenticated, an outbound point-to-point secure and private connection is established between the DS200 and the back-end communications host. Once this secure and private connection has been established, a small, encrypted and digitally-signed unofficial election results bundle is transferred to the back-end communications host at the central reporting location. This file transfer takes only a few seconds, and once complete, the modem is reset to a deactivated status.