ES&S LAYERS OF SECURITY

1. Physical Controls
Physical Security of the voting system is paramount. The Electionware PCs should be kept in a controlled environment that limits physical access to the system. All voting equipment should be outfitted with wire and paper seals.

2. System Hardening
Hardening of the Electionware PC. Among other things, the hardening process locks down what applications can be run and loaded on the PC and establishes user login credentials and roles. It essentially turns the PC into a single use device, dedicated to the sole purpose of creating and operating elections.

3. User Authentication
No matter the device, all election PC’s and voting equipment require login credentials before operation can commence. All failed login attempts are logged.

4. Encryption
All data in motion – such as election media that is moving from the Electionware PC to a voting device – is encrypted. The encryption key is different for each election and is transferred to the voting device separately from the election media. In other words, a different key is used for each election, and the key and the padlock never travel in the same package.

5. Data Integrity Validation
A number of checks are performed when attempting to unlock election media that is loaded in a voting device. These include digital signatures and hash checks to ensure data integrity.

6. Audit Logs & Trails
All actions performed in the election – regardless of the device being used – are logged in detail. All audit logs from voting devices in the field are combined in a single database on the Electionware PC. This database can be searched by device, time, and type of action. All actions performed on the Electionware PC are also logged by user.