DS200 TABULATOR SECURITY FACTS:

Physical and System Access Controls

The DS200 utilizes physical and system access controls including lockable doors, tamper-evident seals and access codes. These security safeguards cannot be bypassed or deactivated and alert election officials of unauthorized access while the unit is in storage, transport, preparation and operation.

Audit Logs

The DS200 generates a detailed audit log of all actions and events that have occurred on the unit, which can be printed at any time. Every action and event, including access attempts, access of system functions and errors, is logged and timestamped.

Proprietary Flash Drives

The DS200 will only accept certified and approved USB flash drives that contain encrypted data sealed with the correct, FIPS-compliant, signed data key. As such, once an election official installs election programming, it is not possible for a separate device to interface with the DS200 in order to overwrite or change the election definition or system firmware.

System Application Controls

The DS200 is a purpose-built tabulator. Its system functions are only executable 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 alerts election officials of errors or changes to the system before any election data is introduced.

Encryption, Hash Validation and Digital Signatures

All data generated during the polls is encrypted and digitally signed. Additional hash validations ensure data integrity remains intact. The DS200 also generates a signed data key, ensuring that should unauthorized access of a unit occur, no other units can be affected through data transfer.