Section 3 – Polling Place Scanners (PPS)

File 3-2 PPS Validation

3.2 Describe any software/firmware validation tools built into the device for use in installation, pre-election, and post-election testing to verify that software/firmware has not been modified.

Democracy Suite integrates a role-based access control system for all software and hardware components. Each user accessing the system is the member of one of the predefined or custom-made roles. Each role has its own set of permissions, or actions that users of that role are allowed to perform. This access control approach provides authentication and authorization services and can be granular according to the jurisdiction’s needs and organization. Complete user and role membership management is integrated within the Democracy Suite EMS Election Event Designer client module.

Further, the ImageCast Precinct protects against unauthorized access or loading of malicious firmware by requiring two-factor authentication for all technician and pollworker menus. In order to gain access, a user must have a valid iButton and enter an authorized username and password.

As previously detailed, all products in the Democracy Suite platform follow best software and application development practices, including additional source code quality and security procedures. All software programs satisfy recommended coding standards, as well as code styling guidelines as required by EAC VVSG standards. Automated code review processes are in place, that verify compliance with industry accepted coding standards for programming languages. In addition, proper system and software hardening procedures are clearly defined and regularly tested. Testing is performed on the lower source code level using code analysis tools, and at the system level using Nessus vulnerability testing tool. Data integrity and confidentiality is implemented according to NIST defined and FIPS validate procedures and algorithms.

All the code is stored in a secure manner within our organization and regularly backed up. Dominion’s IT personnel further improve overall security through the usage of firewalls, intrusion detection/prevention systems, comprehensive employee training, and company-wide security policies. Continuous integration is performed on a daily basis along with in-depth testing, which maintains constant code quality. Documentation covers recommended secure configuration scenarios from securing host operating systems (by using antivirus software, firewall configuration, hardening scripts, performing regular updates, and being in an isolated environment) through encryption of application communication mechanisms, hard disk encryption, and election file encryption. Voting locations are physically secured by trained professionals, machines (tabulators) are locked down from modification through the use of appropriate seals and are uniquely identifiable by having appropriate certificates stored for use in authentication.

Dominion uses multi-level assurance and quality control processes to ensure that all elements of our integrated voting system perform properly with every use. Internal acceptance testing is performed on each voting system on receipt from the manufacturer. By the time our products are purchased by the customer, they have gone through three full rounds of acceptance testing. Independent reviews of election databases are conducted to prior Logic and Accuracy testing. We recommend (and support our customers to conduct) precinct-level pre-election testing.

In addition to this rigorous testing and control program designed to catch errors, Dominion Voting regularly conducts process audits of our acceptance testing, and programming processes to ensure that errors never occur.